OCTOBER 2025

SAPinsider

RESEARCH REPORT

Cloud and AI Security for SAP

Robert Holland

RESEARCH PARTNER

SAP

SPONSORED BY

DataRobot

ONAPSIS

Security Bridge

Executive Summary

Most SAP customers are now running at least some enterprise systems in the cloud. At the same time, organizations are exploring ways to incorporate AI into their enterprise workloads. This convergence of technologies is hugely important from a security standpoint and raises questions about how organizations are planning on securing their expanding cloud footprints while ensuring that their use of AI is protected. In addition, the expanding use of AI to both protect systems as well as defend against attacks is both complicating, while potentially streamlining, the task of protecting cloud-based systems and AI workloads from attack.

To provide insights into the cloud and AI security strategy for SAP systems, SAPinsider surveyed its community between July and October of 2025. To gain additional insights into where respondents stood when it came to securing their cloud and AI environments, four questions in the survey were used to help gauge respondent maturity. This assessment started by seeking

to understand the current security model used for SAP workloads deployed in cloud or hybrid environments. Answer choices included having no specific cloud security model in place, basic perimeter and access control policies only, advanced, risk-based security posture with automated threat response, integrated cloud-native security controls and monitoring, and standardized security policies for SAP cloud workloads.

Respondents were also scored on how artificial intelligence (AI) or machine learning (ML) tools were being used to secure SAP environments. Respondents could choose between having broad, AI/ML adoption as part of intelligent security fabric, integrate AI/ML tools into security operations, using AI/ML in select areas, exploring or piloting select tools, or not using any AI/ML-based security tools.

Lastly, respondents were asked about the capabilities they had in place to manage identity access across SAP cloud and hybrid environments and the frameworks or standards being aligned with SAP security architecture. The more capabilities in place or frameworks being aligned the higher the score. Answer choices included capabilities like integration with identity providers, role-based access controls, and cross-system identity federation and SSO. Similarly, respondents were asked whether they were aligning with the SAP security baseline, ISO 27001, NIST, zero-trust architecture, and CIS controls frameworks.

Respondents with the highest scores were more likely to have integration with identity providers, role-based access controls, and cross-system identity federation than other respondents, have an advanced, risk-based security poster or integrated cloud-native security controls, be integrating AI/ML tools into security operations, and are aligning with three or four different security frameworks. These security leaders represent 20% of respondents.

Those beginning their security journeys mostly had no specific cloud security model in place, were not using any AI/ML-based security tools, usually only had one capability when it came to managing identity access across cloud and hybrid environments, and often did not follow any security frameworks or standards but ISO/IEC 27001. These respondents represented 28% of all respondents. The remaining 52% of respondents represent a majority group.

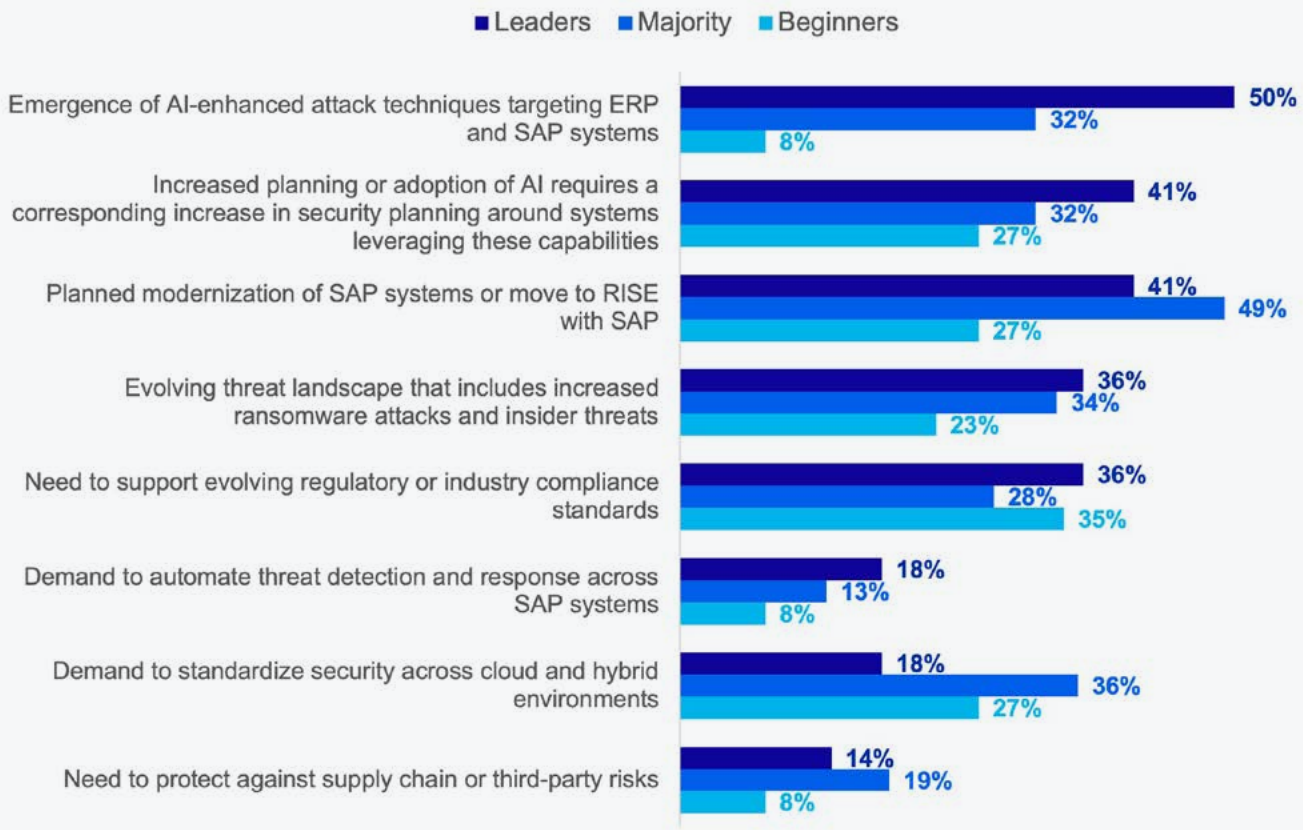
In exploring the factors most responsible for influencing cloud and AI security strategy for SAP systems, the differences between these respondent groups were significant **(Figure 1)**. For example, more than half the leaders reported that their strategies were most impacted by the emergence of AI-enhanced attack techniques targeting ERP and SAP systems. Meanwhile, the majority group were still focused on tasks like ERP modernization and a demand to standardize security across cloud and hybrid environments. These are factors that are of lesser importance to leaders, reflecting the fact that leaders are more likely to have already addressed these concerns or are on their way to completing modernization plans.

50%

of security leaders are concerned about the emergence of AI-enhanced attack techniques

FIGURE 1

Factors Most Responsible for Influencing Cloud and AI Security



Those just beginning their security strategy were most impacted by the need to support evolving regulatory or industry compliance standards. This was followed by the demand to standardize security across cloud and hybrid environments, the planned modernization of SAP systems, and the fact that increased adoption of AI requires an increase in security planning around systems leveraging these capabilities.

This year has seen a significant increase in both the number of attacks targeting SAP systems and in the number of critical vulnerabilities reported and patched by SAP. This increase reflects the fact that accessing SAP systems, and particularly the data stored in those systems, is highly desirable for threat actors. With the AI boom, finding tools that can help accelerate attacks and provide an increased likelihood of success is becoming much easier for these actors. Even if these tools simply help improve the quality of emails or messages used in social engineering attacks, that can have a major impact on success rates.

Coupled with the fact that threat actors are likely to be sharing information, as was probably the case with the zero-day vulnerability discovered in April 2025 where significant numbers of SAP sys-

tems had already been compromised before the issue was even reported, SAP systems are increasingly vulnerable. It is thus no surprise that security leaders are concerned about the emergence of AI-enhanced attack techniques targeting ERP and SAP systems. Because their systems are running in the cloud, this may make them more vulnerable to certain attack vectors.

Ensuring the support of evolving regulatory or industry compliance standards is the most important factor influencing those just beginning to create their cloud and AI security strategy. While important, and this importance is reflected by the fact that security leaders are just as likely to be impacted by this factor, the fact that this exceeds the importance of other factors like the emergence of AI-enhanced attack techniques, the evolving threat landscape that includes increased ransomware attacks and insider threats, and even the planned modernization of SAP systems or the move to RISE with SAP reflects just how far some of these organizations need to go in their cloud and AI journey.

The majority group reported that they were most impacted by the planned modernization of SAP systems and a demand to standardize security across cloud and hybrid environments. This shows that these respondents, while progressing on their cloud journeys, are most likely to still be using systems like SAP ECC either in local environments or in an infrastructure-as-a-service environment following a lift and shift to the cloud. They have most likely not completed more significant modernization. Another factor impacting their cloud and AI security strategy is the need to implement more standardized security practices in these newer cloud environments. Reported at twice the rate of security leaders, this is another way in which it is clear that these respondents have commenced their cloud journey, but are still addressing some more basic cloud security needs.

Just as there were differences between the respondent groups when it came to the factors impacting their security strategy for cloud and AI, there are also differences in the owners of that strategy **(Figure 2)**. For security leaders, the groups most likely to be involved in the ownership of cloud and AI security strategy are the cloud infrastructure or platform team and CIOs or executive leadership. However, the margin over the majority of respondents is only relatively small for both these groups reflecting that these are common groups to be owning this strategy.

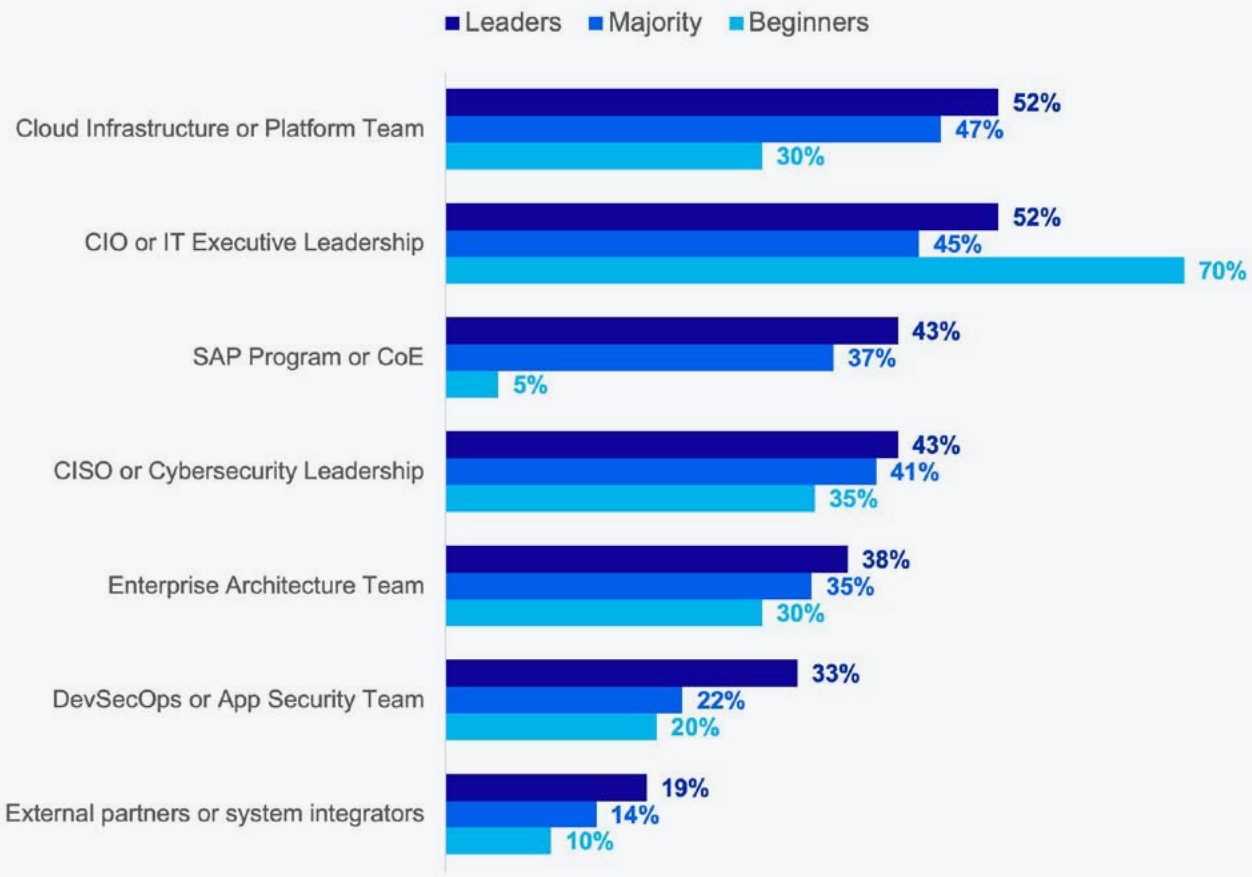
INSIDER
PERSPECTIVE

"Our cloud security strategy was driven by a need to comply with EU regulations, concern about building customer trust, and the reality of running SAP solutions on a hyperscaler. This included ensuring that we used and understood SAP's shared responsibility model. With the increase in cybersecurity attacks, we added layers to our security models including zero-trust, always-on encryption, and continuous monitoring. As we move more SAP workloads to the cloud, we will continue to monitor whether we need to add more to our security approach."

SAP SECURITY LEAD,
CONSUMER GOODS COMPANY

FIGURE 2

Owners of SAP Cloud and AI Security Strategy



What is notable is that there is a much bigger percentage difference between leaders and the cloud majority for the involvement of the DevSecOps or app security teams. These teams are 50% more likely to own cloud and AI security strategy for leaders than for the majority based on an 11% difference between the two respondent groups. The fact that leaders were more likely to report their cloud infrastructure or platform teams, SAP COE teams, or DevSecOps teams were more likely to own the SAP cloud and AI security strategy is actually more reflective of these teams existing in these organizations than in the majority or, especially, with cloud and AI beginners.

70%

of beginners report their security strategy is owned by IT leadership

The fact that these organizations likely do not exist yet for cloud and AI beginners is represented most strongly in the fact that only 5% of beginners said that the SAP program or COE teams were likely to own the cloud and AI security strategy for SAP compared to 43% of leaders and 37% of the majority group. The only way that this would be true is if beginners have not yet created a SAP COE team, or if this team is not focused at all on cloud efforts.

In addition, beginners are also far more likely to focus on having CIOs or IT executives involved in leading their cloud and AI security strategy for SAP than other respondent groups. While these executives are heavily involved for both leaders and the respondent majority, it is at nowhere near the same level as for beginners. This again reinforces the likelihood that teams like cloud infrastructure and DevSecOps have either not yet been created or are yet to switch their focus to cloud operations.

Both beginners and the majority can look at these results and learn from leaders as to where they should be establishing ownership of cloud and AI security strategy for SAP. If these groups do not currently exist or are not involved in these tasks, such as the SAP COE with cloud beginners, there is an opportunity to engage these teams to ensure that an SAP-focused perspective is being included in the future.

For the owners of cloud and AI security strategies there are major challenges, particularly those associated with using AI in SAP-related operations. Even if organizations are not yet embedding AI in their SAP operations, there are some crucial concerns: data quality and availability; complexity of integrating AI that isn't embedded, conforming with regulatory frameworks and ensuring that sensitive data is not exposed; and effectively monitoring models. Customers at different levels of maturity are approaching these needs in different ways as seen in **Figure 3**. While customers have more limited insight into SAP solutions like Joule, there are steps that users at all levels of maturity should be taking.

40%

of leaders are implementing human oversight for AI-driven decisions

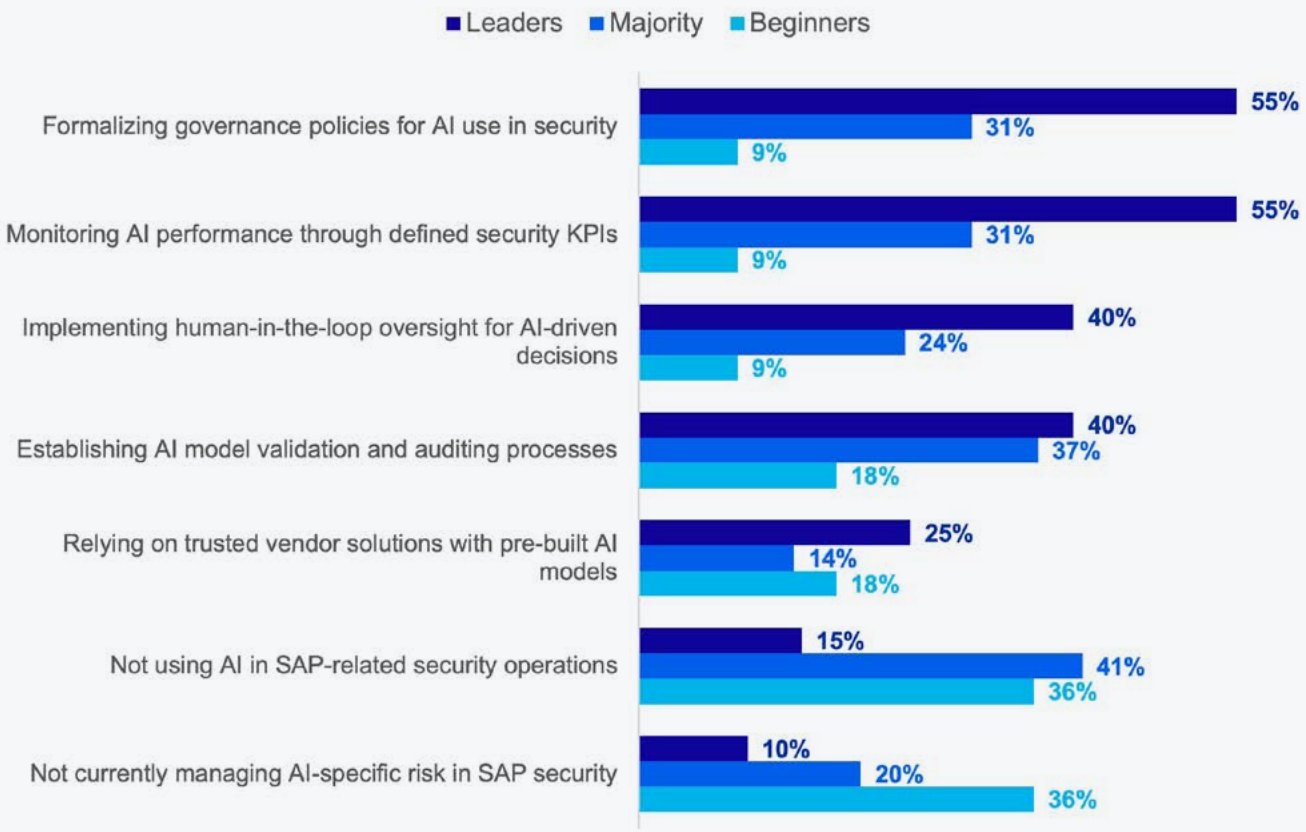
INSIDER
PERSPECTIVE

"We were able to achieve the most progress in creating a strategy for securing our SAP systems in the cloud when our SAP Basis and information security teams collaborated with the business owners in a security oversight group. We aligned the controls we were using, change management processes, and how we should respond to incidents around our business processes. The benefits we experienced included the ability to deploy updates more quickly, fewer audit findings, and clearer accountability across teams."

IT DIRECTOR, MANUFACTURING COMPANY

FIGURE 3

How Risk Associated with Using AI in SAP-Related Operations is Being Managed



The most obvious difference between leaders of a cloud and AI security strategy and the majority of respondents is that leaders are highly likely to be formalizing governance policies for AI use in security as well as monitoring AI performance through defined security KPIs. AI governance is a key part of any AI strategy and putting effective governance in place involves clearly defining ownership, ensuring data quality, and ensuring strong security and access control is in place. By formalizing these governance policies, particularly in the area of using AI for security, leaders are ensuring that they can better manage AI in their organizations moving forward. Formalizing governance policies combined with monitoring AI performance through defined security KPIs will help leaders keep a much better handle on the AI that is both being used within applications and to help protect systems.

In contrast, the majority are either not using AI in SAP-related security operations or are in the process of establishing AI model validation and auditing processes. This difference in focus is primarily due to the fact that these respondent organizations are less advanced in their adoption of AI both in SAP applications and for security purposes. However, nearly a third of these respondents are also working to formalize governance policies for their use of AI in security or are already starting to monitor

AI performance through defined security KPIs. This shows that these organizations are moving towards the activities leaders are already largely engaged in.

Unsurprisingly, beginners are most likely to either not be using AI in SAP-related security operations or are not currently managing AI-specific risk in SAP security. This is almost certainly due to their lack of progress in cloud and AI adoption in general. However, smaller numbers of beginners are in the process of establishing AI model validation and auditing processes or are starting to rely on trusted vendor solutions with pre-built AI models. While the reliance on vendor solutions with pre-build models is also a step being taken both my leaders and the majority, it is a less likely approach for these respondents than other activities. This suggests that this is a starting point to managing risk around using AI in SAP security operations and organizations should move from there to establishing AI model validation and ensuring that humans are embedded in the AI decision loop.

Any sort of investment in cloud or AI security must yield results. For leaders, these investments are helping them achieve measurable outcomes such as a reduced number of security incidents, reduced time to patch or remediate SAP vulnerabilities, and increased automation in access control and provisioning **(Figure 4)**. In fact, the only areas in which leaders are not seeing improved outcomes than other respondents are in the aeras of accelerated audit readiness, automated compliance reporting, and fewer audit compliance violations. Although these differences also suggest that leaders may be placing less focus on these outcomes as they had been improved in the past allowing for a greater focus on outcomes like stronger alignment with zero trust and improved collaboration between SAP and cybersecurity teams.

INSIDER
PERSPECTIVE

"We treat AI like any other high-risk workload touching our SAP systems. This means role-based and attribute-based access and masking any PII. We catalog and register any models in use, and ensure that they go through an approval process with our DevSecOps team. By following these steps, particularly ensuring that any AI applications we develop include an employee approval step, we have been able to scale our AI deployment while remaining compliant."

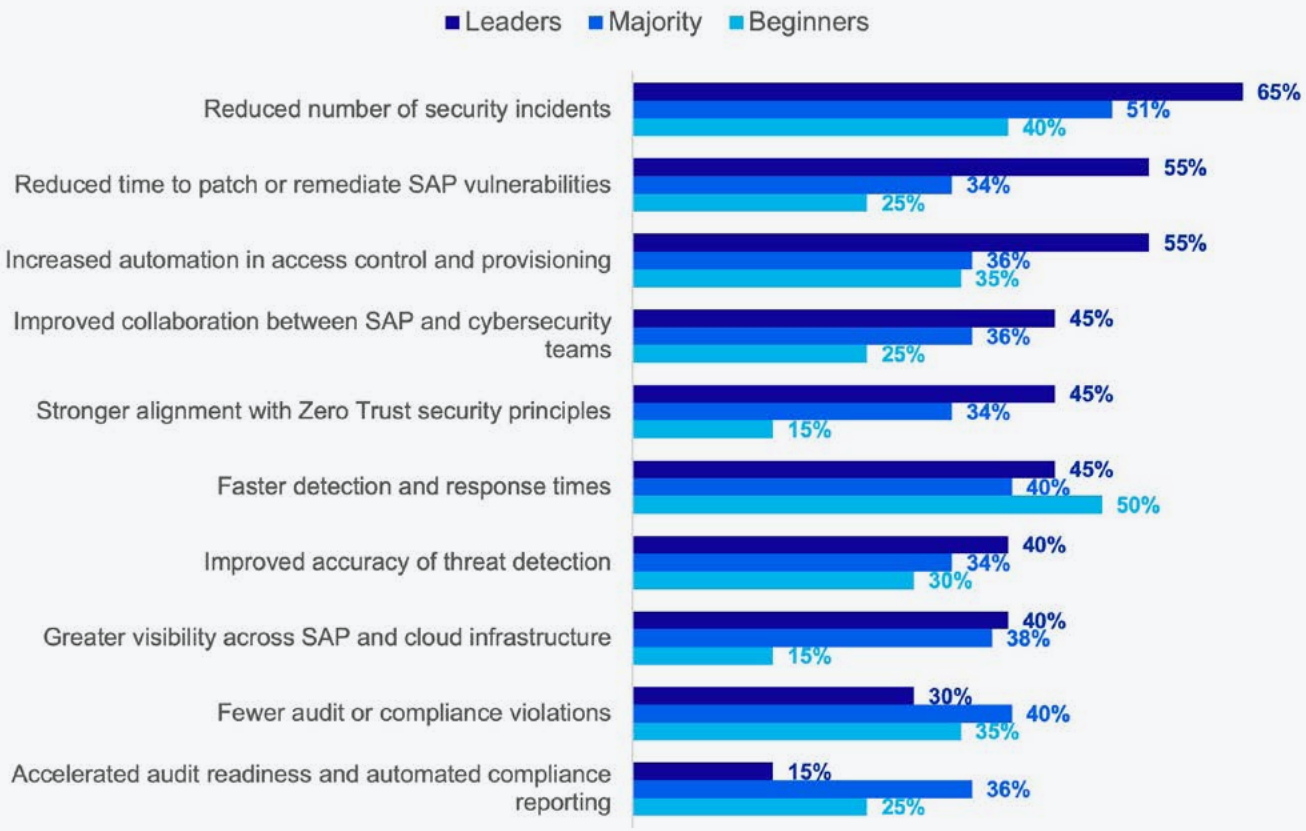
MANAGER, DIGITAL PLATFORMS, ENERGY COMPANY

65%

of leaders have seen a reduction in security incidents after adopting cloud or AI security capabilities for SAP workloads

FIGURE 4

Measurable Security Outcomes Achieved Through Adoption of Cloud or AI Security Capabilities for SAP Workloads



For beginners and the survey majority, there are still benefits to be achieved through the adoption of cloud or AI security capabilities for their SAP workloads. For example, beginners are seeing faster detection and response times which can help ensure that any potential attacks are remediated more quickly as long as the plans are in place to effectively manage those attacks. In addition, the survey majority have experienced improved detection and response times in combination with fewer audit and compliance violations. While these benefits may not be as extensive as those experienced by leaders, these are just starting points that those who are beginning or underway in their cloud and AI journeys can achieve as they work towards greater benefits.

This year's survey also revealed other trends, including the following:

- Leaders identified the European General Data Protection Regulation (85%) as the security or data protection requirement that required the most effort to follow or ensure compliance with in relation to an SAP cloud landscape. For the majority the requirement that required the most effort to follow was Sarbanes-Oxley (49%), while beginners also faced challenges with GDPR (33%). However, a third of beginners (33%) reported that these were not applicable reflecting the possibility that they were not following any data protection regulations.

85%

of security leaders say GDPR requires the most compliance effort

- Respondents identified SAP solutions such as SAP Solution Manager, SAP Focused Run, or SAP Cloud ALM (50%) as the tools they were most likely to use to monitor and detect threats in SAP environments. This was followed by cloud-native security monitoring (48%) such as Azure Sentinel, AWS Security Hub, or Google Security Command Center. However, more than a third (39%) reported that they were still using manual audits and periodic SAP security assessments, although this was disproportionately made up of beginners (41%) or the survey majority (45%) while only 25% of leaders continued to utilize manual audits.

39%

of respondents are still using manual audits to detect threats in SAP systems

- Respondents were most likely to be collaborating with Microsoft (62%), SAP (57%), AWS (42%), IBM (18%), and SUSE (18%) when it came to vendors or partner technologies supporting their SAP cloud and AI security strategy. However, 81% of leaders were utilizing SAP compared to just 52% using Microsoft and 43% using Google Cloud. The majority focused on Microsoft (71%), SAP (65%), and AWS (47%), while beginners primarily utilized Microsoft (55%), AWS (35%), and SAP (20%).

81%

of security leaders are using SAP technologies to support their cloud and AI security strategy

Required Actions

Based on the survey responses, organizations should consider the following when making their plans for cloud and AI security for SAP:

Plan for AI projects and adoption in SAP systems and data even if they are not in use today.

While beginners may not yet be starting AI projects in their SAP environments, and the majority are most likely to be in an evaluation phase, it is vital that all organizations running SAP environments start planning for the inclusion of AI in their SAP systems. While access to generative AI capabilities like Joule are only accessible in SAP S/4HANA Cloud through a RISE with SAP contract, SAP is now starting to build AI-native applications like those announced for SAP Ariba where AI will be embedded in multiple areas in the applications. Over time this will be extended to all line of business applications from SAP, and SAPinsiders will need to be prepared to defend these systems.

Deploy technologies that will help support cloud and AI strategy.

Leaders in the space are already utilizing SAP Business Technology Platform, SAP Identity Access Governance, and SAP GRC solutions in addition to partner solutions such as Microsoft Sentinel, Google Chronicle, AWS Security Hub, and secure Linux platform and container hardening. This is being supplemented with technologies from third-party SAP-specific security platforms which provide additional capabilities beyond those offered from SAP and infrastructure partners. As organizations move to the cloud it is vital that the capabilities be put in place to effectively secure these cloud-based environments and that starts with security frameworks and technologies from different vendors.

Collaborate across organizations to ensure that security strategy for SAP cloud and AI capabilities is effectively managed.

Most respondents (52%) reported that it is their CIO or IT executives that are managing their cloud and AI security strategy for SAP. However, those leading in cloud and AI security are more likely to involve teams such as the cloud infrastructure or platform team or the SAP center of excellence in their organizations. While driving this through the CIO organization is not inherently bad, the best approach is to ensure that teams with the requisite knowledge are collaborating across the organization. This should include the DevSecOps team, application security teams, and enterprise architecture teams beyond infrastructure and COE teams. With each team bringing their expertise to the discussion, organizations can help ensure that cloud-based and AI systems are most effectively protected.

DART MODEL FRAMEWORK

STRATEGY AND NEEDS FOR CLOUD AND AI SECURITY STRATEGY FOR SAP SYSTEMS

DRIVERS

- Emergence of AI-enhanced attack techniques targeting ERP and SAP systems (50%)
- Increased planning or adoption of AI requires a corresponding increase in security planning around systems leveraging these capabilities (41%)
- Planned modernization of SAP systems or move to RISE with SAP (41%)

ACTIONS

- Implementing Zero Trust principles and technologies (50%)
- Training SAP and security teams to operationalize AI tools for ERP-specific use cases (45%)
- Implementing centralized identity and access management (41%)
- Establishing centralized AI-driven observability for SAP and adjacent cloud services (41%)
- Deploying automated threat response tools across SAP cloud and hybrid

REQUIREMENTS

- Cybersecurity tools that provide consistent protection across cloud and on-premise environments (95%)
- Zero trust security principles (91%)
- Automated threat response tools (91%)
- Cross-functional security and SAP collaboration (86%)
- Security training for SAP administrators and developers (86%)
- Regular training and education programs for all employees (86%)

TECHNOLOGIES

- Automated threat detection and response (48%)
- Hyperscaler-native tools (43%)
- SAP IAG or GRC (43%)
- SAP BTP (43%)
- Anomaly detection for user behavior or data access (33%)
- Kubernetes security tools (33%)
- SIEM/SOAR platforms (29%)
- Third-party SAP-specific security platforms (24%)
- Predictive risk scoring (19%)
- AI-driven vulnerability scanning (14%)

APPENDIX | THE DART™ METHODOLOGY

SAPinsider has rewritten the rules of research to provide actionable deliverables from its fact-based approach. The DART methodology serves as the very foundation on which SAPinsider educates end users to act, creates market awareness, drives demand, empowers sales forces, and validates return on investments. It is no wonder that organizations worldwide turn to SAPinsider for research with results.

The DART methodology provides practical insights, including:

DRIVERS	These are macro-level events that are affecting an organization. They can be both external and internal, and they require the implementation of strategic plans, people, processes, and systems.
ACTIONS	These are strategies that companies can implement to address the effects of drivers on the business. These are the integration of people, processes, and technology. These should be business-based actions first, but they should fully leverage technology-enabled solutions to be relevant for our focus.
REQUIREMENTS	These are business and process-level requirements that support the strategies. These tend to be end-to-end for a business process.
TECHNOLOGY	These are technology and systems-related requirements that enable the business requirements and support the company's overall strategies. The requirements must consider the current technology architecture and provide for the adoption of new and innovative technology-enabled capabilities.

REPORT SPONSORS

DataRobot

DataRobot empowers AI teams to deliver the agentic workforce of the future. Our platform enables organizations to create and scale AI agents that integrate directly with business processes — driving efficiency, transforming operations, and delivering real results. With built-in governance and safeguards, we help enterprises deploy AI securely and confidently. As an SAP Endorsed App available on the SAP Store, DataRobot seamlessly integrates with SAP systems to modernize enterprise planning — from foundational predictive models and what-if analysis, to advanced simulation and optimization, to an agentic future where users interact with AI in natural language for real-time scenarios and insights.

For more information, visit **our website** and connect with us on **LinkedIn**.

ONAPSIS

Onapsis is the global leader in SAP cybersecurity and compliance, trusted by the world's leading organizations to securely accelerate their SAP cloud digital transformations with confidence. As the SAP-endorsed and most widely used solution to protect SAP, the Onapsis Platform empowers Cybersecurity and SAP teams with automated compliance, vulnerability management, threat detection, and secure development for their RISE with SAP, S/4HANA Cloud and hybrid SAP applications. Powered by threat insights from the Onapsis Research Labs, the world's leading SAP cybersecurity experts, Onapsis provides unparalleled protection, ease of use, and rapid time to value, empowering SAP customers to innovate faster and securely.

For More information, visit **www.onapsis.com**

SecurityBridge is the leading provider of a comprehensive, SAP-native cybersecurity platform. Trusted by organizations worldwide to safeguard their most critical business systems. Our platform seamlessly integrates real-time threat monitoring, vulnerability management, and compliance capabilities directly into the SAP environment, empowering organizations to protect their data's integrity, confidentiality, and availability with minimal manual effort. With a proven track record, including a stellar customer success rating and over 8,000 SAP systems secured globally. SecurityBridge stands out for its ability to accurately provide a 360° view of the SAP security posture, ease of use, rapid implementation, and transparent licensing. We are committed to innovation, transparency, and customer-centricity, ensuring businesses can confidently navigate the evolving landscape of SAP security threats.

For more information, visit **www.securitybridge.com**

RESEARCH PARTNER

SAP is creating opportunities through learning and development for all with free, self-guided, and premium learning resources, opportunities to engage in the SAP Community and to experience SAP solutions hands-on.

Learn more at **https://learning.sap.com**

SAPinsider

SAPinsider comprises the largest and fastest-growing SAP membership group worldwide. It provides SAP professionals with invaluable information, strategic guidance, and road-tested advice through events, magazine articles, blogs, podcasts, interactive Q&As, white papers, and webinars. SAPinsider is committed to delivering the latest and most useful content to help SAP users maximize their investment and leading the global discussion on optimizing technology.

For more information, visit **SAPinsider.org.**